

REMARKS

I. THE CITED COMBINATION OF REFERENCES CANNOT SUSTAIN A § 103 REJECTION OF THE INDEPENDENT CLAIMS 1, 8, AND 15

Trossen provides for the relocation from a first content source to a second content source when a network layer-level handoff occurs. In contrast, the claimed invention supports a method for transmitting information packets across network firewalls that includes a trusted entity that is provisioned to allow two devices to communicate via a firewall. Because of the vast disparity in these solutions, Trossen and the other cited reference fail to disclose essential claim elements alone or in combination of the claimed invention. Trossen is the sole cited reference for teaching the creation of a pinhole and replacing an address in the address header of an information packet with an address for the communication pinhole port, with paragraphs 0007 and 0024, as well as 0008, cited.

The subject paragraphs read as follows:

[0007] The present invention provides for a relocation of content sources that provide media content to a mobile terminal (mobile node) when a network layer-level handoff occurs. The relocation of content sources enables the mobile terminal to seamlessly execute an application that utilizes the media content from a current content source before the handoff and from a new content source after the handoff. The mobile terminal registers with a current access router in order to inform the access router about application context information. The current access router informs a new access router about the impending handoff. The new access router consequently discovers the new content source.

[0008] In an embodiment of the invention, the network comprises a current access router, a current content source, a new access router, and a new content source. The new access router and the new content source may be associated with a different administrative network domain than the current access router and the current content source. The embodiment supports an Internet protocol (IP) as the network layer, although other embodiments can support other network layer protocols (corresponding to the third layer of the Open Systems Interconnection model). Before an IP-level handoff, the current access router and the current content source provides media content to the mobile terminal. The mobile terminal

registers with the current access router in order to provide application context information that is associated with the application. The current access router informs a new access router in response to an impending handoff. The new access router consequently discovers the new content source, which is able to provide the media content for the application. The new content source consequently establishes an IP path to the new care-of address of mobile terminal, via new access router. When the IP-level handoff does occur, the current content source informs the new content source about the current state of the application in order that the new content source can resume the application in a seamless manner.

[0024] With a state creation procedure 217, new content source 119 configures the new IP path between new content source 119 and new access router 117 (corresponding to the new care-of address) according to states (e.g. QoS level) that are consistent with the media description. QoS establishment along the new path can be done using protocols such as Resource Reservation Protocol (RSVP), or other QoS signaling protocols that are being designed in the Next Steps in Signaling (NSIS) working group of IETF. Configuring the new IP path may also involve creating a pinhole in the firewall that may reside between the new access router 117 and the new content source 119. The new IP path may not be able to support the media description that is supported by the current IP path (current content source 111 to network 113 to current access router 109 to base transceiver station 107). In such a case, new content source 119 may redefine the media description (e.g. modifying the coding format, altering resolution, resizing, and adjusting the degree of motion) and send the modified media description to the new care-of address of mobile terminal via the new access router 117 as part of state creation procedure 217. The communication of new media description may be done using SIP messages. In the embodiment, new access router 117 stores the modified media description (or the corresponding SIP message). New access router 117 subsequently sends the modified media description (or the corresponding SIP message) to mobile terminal 105 in an action 223 when mobile terminal 105 performs the IP-level handoff. In another embodiment, the new access router can send the modified media description (or the corresponding SIP message) to mobile terminal 105 via the current access router 109. Mobile terminal 105 acknowledges the reception of the modified description with a confirmation message 225.

The content source in Trossen originates the media content being transmitted and does not disclose any of the router functionality of the trusted entity as claimed in the invention. This router function is not disclosed, taught, or suggested in Paragraph 007 or 0024 of Trossen or by the “trusted content server” of O’Keefe. Trossen further does not

disclose the creation of a pinhole request or creating a pinhole communication port in the firewall in response to the creation of a pinhole request. Trossen fails to disclose any mechanism for creating a communication pinhole port, including use of a trusted entity, use of create pinhole request, use of create pinhole response, or updating a routing table with the address designation of a communication pinhole port. Trossen only states that “[c]onfiguring the new IP path may also involve creating a pinhole in the firewall that may reside between the new access router 117 and the new content source 119.”

Trossen, paragraph 0024. This statement never discloses, teaches, or suggests any mechanism for creating the pinhole performed by the content source. Concluding that the content source functions in any analogous manner as the trusted entity, requires the Examiner to make impermissible, unsupported assumptions regarding the pinhole creation. *See In re Warner*, 379 F.2d 1011, 1017, 154 USPQ 173, 177 (CCPA 1967), cert. denied, 389 U.S. 1057 (1968).

Trossen actually teaches away from the invention by specifically indicating that a separate access router, not the content source, performs IP-level handoff; implying the access router establishes a new IP path. *Trossen, paragraph 0008.* The current access router performing a handoff to a new access router functions according to well-known prior art mechanisms. *See also Trossen, paragraph 0007* (i.e. “*The current access router informs a new access router about the impending handoff. The new access router consequently discovers the new content source.*”)

Furthermore, there is nothing stated in the RSVP protocol that teaches, suggests, or discloses a specific create pinhole message request or create pinhole message response or any possible role in creating pinholes through firewalls. *See Exhibit 1, RFC: 2205*

“Resource Reservation Protocol”, Braden, September 1997. Concluding that Trossen teaches any of these limitations requires using the invention in hindsight as a guide to impermissibly read into the reference unsupported assumptions on how the IP path is configured, pinholes created, and packets transmitted. See *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988); *Rockwell Int’l Corp. v. United States*, 147 F.3d 1358 (Fed. Cir. 1998); *In re Warner*, 379 F.2d 1011 (CCPA 1967), cert. denied, 389 U.S. 1057 (1968); and *Grain Processing Corp. v. American Maize-Products Co.*, 840 F.2d 902 (Fed. Cir. 1988). Moreover, as previously noted, this handoff is performed by the access router and not the content source. The handoff mechanisms are not accomplished by the content source, so any assumptions or any conclusion as to any alleged role for creating a pinhole or any other claimed routing function should not apply to the content source and instead are exclusive to the access router.

The Examiner appears to believe that numerous claim elements are inherent to various basic teachings of Trossen. However, Trossen does not describe any mechanism or procedure that creates a pinhole or transmits a packet through a firewall. Essential claim elements in Claim 1 include the trusted entity replacing an address in the address header of an information packet with an address for the communication pinhole so the information packet can be transmitted through the pinhole to the communication device. There is no suggestion that the trusted entity in Trossen replaces an address in an information packet. Because the content source is the origin of the information packet in Trossen (see paragraph 0019), Trossen cannot inherently teach replacing an address in the address header with an address for the communication pinhole. To the contrary, the proper inherent teaching is that the content source cannot and never replaces an

original addresses. Trosson's content sources cannot replace the information packet according to the claimed mechanism.

Claim 8 requires 1) receiving a create pinhole request at the trusted entity, 2) creating a pinhole communication port in the firewall in response to the create pinhole request, 3) receiving a first information packet at the trusted entity to be transmitted across the firewall through the pinhole, and 4) replacing an address in the information packet address header information with a communication port address for the created pinhole. The RSVP protocol cited by the Examiner fails to teach any messages or procedures relating to firewalls or pinholes (*See Exhibit 1*), therefore receiving a pinhole request and creating a pinhole in response at the trusted entity cannot be taught by Trossen. Since the content source in Trossen creates the information packets received by the network, it is impossible for the content source to receive an information packet to be transmitted across the firewall or replace an address in the information packet.

Claim 15 requires 1) providing a routing table on the trusted entity with the address designation for the pinhole communication port and 2) receiving a packet transmission at the input of the trusted entity to be sent to a communication device inside the communication network. These two claims are simply not taught by Trossen. There is no discussion relevant to routing tables maintained on the content source in Trossen, and the content source may or may not have a routing table with the address designation for the pinhole port. It is simply improper to conclude that the content source must have a routing table with the address designation for the pinhole port, because a content source does not inherently possess a router table and an intervening router maintaining the address is a more likely assumption. Furthermore, as the source creating the data stream,

it is impossible for the content source to receive a packet to be sent to communication device.

Also, O'Keefe is cited as support for a trusted entity (i.e. O'Keefe's trusted content server), which the Examiner admits is not taught in Trosson. However, the trusted content server in O'Keefe does not perform any router functions or have any role in creating pinholes in a firewall. O'Keefe does not teach, suggest, or disclose a trusted entity as claimed, because it fails to function as a router to replace packet addresses or maintain a routing table. It apparently functions to create and transmit information packets derived from documents collected from databases and verified by a separate verification server and does not make any address substitutions (i.e. it is the source of the IP packets).

These claims are simply not taught by the cited references, which rely upon Trossen to disclose the routing functionality by the trusted entity, but as noted, Trossen's content source does not perform analogous routing which can only be done by separate access routers. The content sources in Trossen create packets, which makes it impossible to receive a packet to transmit to the pinhole or replace an address in the packet header with an address for the pinhole communication port. There is no suggestion within the references that the content sources in Trossen have any role in creating pinholes, and none of the cited references teach, disclose, or suggest any procedure or exchanged messages for creating a pinhole. O'Keefe also fails to disclose any of the claimed routing functionality or a trusted entity as claimed, so the two references cannot sustain a § 103 rejection.

II. CONCLUSION

The claims are distinguishable from the teachings of the cited references. The Applicant believes that the arguments presented traverse the Examiner's 35 U.S.C. § 103 rejection. Independent claims 1, 8, and 15 are allowable because the cited reference fail to combine and disclose, teach, or suggest a trusted entity able to function as claimed. Since the dependent claims add further limitations to the allowable independent claims, the Applicant believes the dependent claims are likewise allowable. Accordingly, pending claims 1-20 are believed allowable because the claimed invention is not disclosed, taught, or suggested by the cited reference.

It is believed that no additional fees are necessary for this filing. If additional fees are required for filing this response, then the appropriate fees should be deducted from D. Scott Hemingway's Deposit Account No. 501,270.

Respectfully submitted,



Malcolm W. Pipes
Reg. No. 46,995
Attorney for Applicant

Hemingway & Hansen, LLP
Comerica Bank Tower, Suite 2500
1717 Main Street
Dallas, Texas 75225
(214)292-8301 (voice)
(214)739-5209 (fax)